China Uses Unencrypted Websites to Hijack Browsers in GitHub Attack

By Bill Budington

Published: 2015-04-01 · Archived: 2026-04-05 18:50:29 UTC

Update 2015-04-02: Robert Graham over at Errata Security has published some excellent research pinpointing the routers responsible for the attack, which seems to confirm their location within the Great Firewall of China.

Over the past few weeks, China has been using its country's Internet infrastructure to attack political opponents by turning normal users' web browsers into Denial of Service tools. These attacks were a deep violation of the basic trust that allows the Internet to function smoothly, and an disquieting and unprecedented development in the history of state-orchestrated denial-of-service attacks. They exploited the fact that many enormous sites still use insecure HTTP rather than HTTPS, allowing the Great Firewall to modify those sites, and the fact that our web browsers are willing to run JavaScript code on an extremely liberal basis. These facts allowed China to marshal an incredible number of "zombie" systems both inside and outside of China, making billions of requests in an attempt to overwhelm the targets' servers.

The attack targets code-hosting platform GitHub, and URLs used in the attack point to two repositories, greatfire and cn-nytimes, which mirror GreatFire.org and the Chinese New York Times. As an analysis published by researchers at Netressec explains, this Man-on-the-Side attack modifies the Baidu Analytics JavaScript included by many sites to inject a malicious copy. The malicious version of the JavaScript instructs browsers to make frequent requests to the two GitHub URLs. As long as a browser remained on the Baidu Analytics-including site, it would continue generating traffic at a regular interval. It is important to note that although China is using its privileged access to backbone routers within its borders to modify the Baidu resources, it is ultimately end users anywhere in the world who run the malicious code who are having their browsers hijacked.

GitHub has announced that this is the largest DDoS that they have ever dealt with. Despite the scale of the attack, neither GitHub nor the individual repositories have been forced offline. In fact, due to GitHub's wide deployment of HTTPS, it would be quite hard for China to censor these specific endpoints without censoring the entirety of GitHub. One of the advantages that HTTPS provides is that it not only encrypts the contents of a web page, but also the specific URL of the page being requested. Unless you have access to the private keys for a given site, it is difficult for an attacker to determine exactly which URL within a site is being accessed in a secure browsing session. And if the attacker can't determine which requests are for pages they want to block, they are forced to block the entire site if they want to prevent access to certain pages.

This is a big advantage for citizens who wish to access information freely within a censorship regime. In order to mitigate the risk of critical information being censored, content creators can mirror their data on a secure domain that the censors may be reluctant to block for fear of political or financial consequences. It seems that that is exactly what has happened in this situation. Before the GitHub attack started on March 26th, GreatFire.org reported an attack on their own servers starting March 17th. And indeed, blocking GitHub would have injurious

effects on Chinese coders and thus the Chinese economy. When China previously blocked the site for days at a time in January 2013, the former head of Google's China operations Kai-Fu Lee posted on the micro-blogging site Sina Weibo that the act was "unjustifiable," and that it "will only derail the nation's programmers from the world, while bringing about a loss in competitiveness and insight." This time, they've gone a step further and actually weaponized Chinese Internet businesses in order to censor critical voices.

We know that China injected the payload at some point between Baidu's servers and when the traffic exited the country. This was only possible due to the fact that the Baidu Analytics script included on sites is not using encryption by default. Without HTTPS, anyone sitting between the web server and the end user can modify content arbitrarily. This is part of the reason we need 100% deployment of HTTPS for the entire web. At the same time, It's important to note that HTTPS isn't a complete inoculation against malicious state action. The government of China could easily have leaned on Baidu to provide their encryption keys to the censors to incorporate in their Man-on-the-Side attack. Alternatively, they could have forced Baidu to deliver the malicious code directly from their servers. And as we have pointed out before, when governments can force web services to fork over their crypto keys or suffer the consequences, an enormous amount of information about end users activities is divulged. In this case, it's worse: governments can turn people across the world into unwitting partners in assisting censorship regimes to stifle free speech.

China isn't unique in its technical capacity to inject traffic. Most national governments could apply this same technique, if they host popular JavaScript within their borders and have the tools to modify Internet traffic leaving their country. It has become increasingly common for websites to include utility libraries and ad networks hosted on a diaspora of servers across the globe. Any one of these third party resources can modify page content, divulge browsing habits, or initiate an attack like the one we've described.

The solution is twofold: technical and political. As a site maintainer, you can host utility libraries locally. That way, a compromise of one remote resource will not result in malicious JavaScript being executed by your users. In this instance, using open alternatives for analytics would have averted users loading remote attack code. Sysadmins can deploy HTTPS, making it harder for malicious agents to modify traffic in-transit. And citizens can support initiatives such as the Manila Principles, which seeks to establish a clear legal framework around content restriction, one that respects human rights and is grounded in due process and backed by international law. Only a combination of sane policy and technical measures can limit governments' power to hijack our browsers and use them to censor the Internet worldwide.

2015-04-01: updated first paragraph for a slightly less technical introduction.
